IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
EASTERN DIVISION

Case No. 4:20-cr-81-M

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>ANTHONY JOSEPH FRITZINGER,<br><br>Defendant. | ORDER |

This matter comes before the court on Defendant's Motion to Suppress Evidence [DE 71]. Defendant challenges the constitutionality of two warrants, one authorizing the search and seizure of his electronic devices and the other requiring the disclosure of activity logs and private communications associated with his social media accounts. Defendant also challenges the warrantless search of internet protocol ("IP") logs pertaining to his various social media accounts and email accounts. Lastly, Defendant moves in limine to exclude screenshots as inadmissible hearsay under the Federal Rules of Evidence. For the following reasons, the motion is denied.

## I. Background

### A. Factual Background

On April 21, 2020, Special Agent Peter Salomon ("S/A Salomon") of the Naval Criminal Investigative Service ("NCIS") obtained referral information indicating that Defendant Anthony Fritzinger ("Fritzinger"), a Lance Corporal in the United States Marine Corps at the time, was committing the offenses of possession of child pornography, extortion, and solicitation of minors. The information specifically indicated that Fritzinger was soliciting and receiving sexually explicit photographs from minors through social media. Fritzinger would also threaten to disseminate the

photographs he had obtained to third parties unless the minors provide him additional photographs. S/A Salomon later requested several warrants and subpoenas to further the investigation into the suspected offenses.

***i. CASS Warrant***

On April 27, 2020, S/A Salomon applied for a Command Authorization for Search and Seizure ("CASS Warrant"). He sought authorization to search and seize, in relevant part, Fritzinger's cellphone and any "additional electronic devices" contained in Fritzinger's "barracks room [and] car" for evidence of possession of child pornography, extortion, communication of threats, and solicitation of minors. *See* DE 71-2 at 1.

The affidavit supporting his application indicated that, on February 22, 2020, one of the victims of Fritzinger's suspected extortion scheme reportedly received several direct messages on Instagram from three different usernames. One message demanded "nude pictures . . . or else other nudes already in [his] possession would be sent to everyone she knows." *See id.* at 4. She did not send any photographs. Within a few minutes, the victim received another message from a second username stating "[s]end or those friends of yours will be the first to get these nudes." *Id.* As before, she did not send any photographs. The victim's friend then received a nude photograph of the victim from a third username. The photograph depicted the victim when she was sixteen years old. She realized it was the same image she had sent to Fritzinger when she had an online relationship with him a few years ago. The affidavit stated that there was additional evidence of similar conversations with other victims who had not yet been identified.

Based on the available information, S/A Salomon believed that Fritzinger's electronic devices would likely contain "IP addresses, connections history, applications" and other information indicating whether the known extortionate messages and sexually explicit material originated from one of his devices. *Id.* at 5–6. He believed the illicit material "received as a result

of these conversations" and "used as leverage may exist on the electronic devices under [Fritzinger's] control." *Id.* He also believed Fritzinger's cellphones, laptops, and other electronic devices would have the capacity to transfer and store "large quantities of data." *Id.* S/A Salomon stated the devices were "extremely vulnerable to tampering or destruction (both from external sources as well as from destructive code imbedded in the system), [so] a controlled environment is essential to [the devices'] complete and accurate analysis." *Id.* at 6.

The CASS Warrant returned at least one laptop and two SD memory cards. One memory card contained multiple sexually explicit photographs appearing to depict female minors and screenshots of social media profiles of females ranging from approximately thirteen to twenty-one years old. DE 71-5 at 1. The other memory card stored numerous images from a video chat depicting a possible minor exposing her genitals. *Id.* at 3.

***ii. Investigative Subpoenas***

About a month after executing the CASS Warrant, S/A Salomon requested subpoenas requiring Snap [DE 71-7], Google [DE 71-9], and Facebook [DE 71-10] to disclose IP logs and other subscriber information relating to numerous social media accounts and email addresses that appeared to belong to Fritzinger. S/A Salomon stated in his subpoena requests that he linked Fritzinger to the targeted accounts and email addresses after reviewing the contents of Fritzinger's cellphone and the information provided by the police department that originally referred the case to NCIS. *See, e.g.*, DE 71-7 at 2. Each subpoena returned pages of information pertaining to the login requests for each named account/address, including the date, time, and IP address requesting access to the accounts/email addresses. *See, e.g.*, DE 71-8; DE 71-11.

***iii. Instagram Warrant***

On June 17, 2020, S/A Salomon applied for a second warrant ("Instagram Warrant") targeting seventeen Instagram usernames that were implicated in the extortion scheme for evidence

of child pornography possession, extortion, and solicitation of minors. First, S/A Salomon sought to require Instagram to disclose, in relevant part, (1) "activity logs including IP logs and other documents showing [access times]" since the creation of the underlying accounts; and (2) "communications and other messages sent or received by the account[s]" during the time of the suspected extortion scheme, specifically between June 4, 2018 to April 28, 2020. DE 70-7 at 14. Once Instagram returned the required disclosures, he sought to seize evidence relating to the commission of the suspected offenses, including "how and when the Instagram account was accessed or used," "the chronological and geographic context of account access, use, and events relating to the [suspected offenses]," and "the Instagram account owner's state of mind" in relation to the suspected offenses. *Id.* at 15.

The affidavit supporting these requests explained that S/A Salomon identified the targeted usernames after reviewing the contents of Fritzinger's cellphone and the referral information. *See id.* at 5. Based on the content associated with the usernames and the fact that Fritzinger's cellphone had access to these usernames, S/A Salomon believed the usernames belonged to Fritzinger. *Id.* S/A Salomon then explained that Fritzinger had used similar usernames to solicit child pornography from several victims. *Id.* at 3–6. He explained the electronic "information stored in connection with an Instagram account may provide crucial evidence . . . of the criminal conduct under investigation." *See id.* at 6–10.

**B. Procedural Background**

On September 2, 2020, the United States indicted Fritzinger on one count of manufacturing child pornography, in violation of 18 U.S.C. § 2251(a) & (e); one count of possession of such material, in violation of 18 U.S.C. § 2252(a)(4)(B); and two counts of using the internet to promote an extortion scheme, in violation of 18 U.S.C. § 1952(a)(3). DE 1. The United States has since superseded those charges. DE 84 (second superseding indictment). In addition to the original

counts, Fritzinger now faces four counts of enticing a minor to engage in illegal sexual conduct, in violation of 18 U.S.C. § 2422(b); and four additional counts of manufacturing child pornography, in violation of 18 U.S.C. § 2251(a) & (e). DE 84. Trial is currently scheduled to begin on September 9, 2024. DE 87.

On January 22, 2024, Fritzinger filed the instant motion to suppress, which seeks to exclude evidence obtained from his electronic devices, social media accounts, and email addresses based on purported Fourth Amendment violations. DE 71. Fritzinger also requests to exclude certain screenshots under Rule 802 of the Federal Rules of Evidence. *See id.* The United States responded on February 12, 2024. DE 75. Fritzinger timely replied. DE 79. Neither party has requested an evidentiary hearing in connection with this motion, nor does the court find such a hearing necessary for the fair disposition of the instant motion because the parties do not genuinely dispute any of the material facts related to the issues at bar. *United States v. Griffin*, 811 F. App'x 815, 816 (4th Cir. 2020). The court is therefore fully apprised.

## II. Discussion

The motion concerns alleged violations of the Fourth Amendment, which provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *See* U.S. Const. amend. IV. The Supreme Court has "repeatedly affirmed" that "the ultimate touchstone of the Fourth Amendment is reasonableness." *Heien v. North Carolina*, 574 U.S. 54, 60-61 (2014).

Fritzinger challenges the particularity of both warrants in this case. The CASS Warrant authorized the search and seizure of the "electronic devices" contained in Fritzinger's barracks room and vehicle, and the Instagram Warrant required Instagram to disclose all activity logs and a time-limited portion of communications associated with seventeen usernames linked with the

extortion scheme. Fritzinger argues that both warrants lack reasonable specificity given the nature of the devices and information and the context of the investigation.

Fritzinger also challenges the constitutionality of the subpoenaed disclosures of the IP logs associated with his social media accounts and email addresses, contending that he maintained a legitimate privacy interest in the subpoenaed information, so the disclosures constituted warrantless searches in violation of the Fourth Amendment. Lastly, he argues the court should exclude in limine any screenshots revealing the age of his alleged victims because those statements constitute inadmissible hearsay under the Federal Rules of Evidence. The court discusses each of Fritzinger's arguments in turn.

**A. Particularity Requirement**

"[A] warrant may satisfy the particularity requirement *either* by identifying the items to be seized by reference to a suspected criminal offense *or* by describing them in a manner that allows an executing officer to know precisely what he has been authorized to search for and seize." *United States v. Blakeney*, 949 F.3d 851, 863 (4th Cir. 2020). "By limiting the authorization to search to the specific areas and things for which there is probable cause to search," the Fourth Amendment "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). Failure to reasonably limit the scope of the authorized search to the specific areas and things for which probable cause exists amounts to impermissible overbreadth. *See, e.g.*, *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006); *United States v. Manafort*, 323 F. Supp. 3d 795, 801 (E.D. Va. 2018).

***iv. CASS Warrant***

Fritzinger seeks to suppress several electronic devices, including several laptops and memory cards, which law enforcement searched and seized pursuant to the CASS Warrant. *See*

DE 71 at 5–7. He argues the CASS Warrant "was overly broad" because it "did not attempt to precisely define what items were to be seized beyond the term 'electronic devices.'" *Id.* at 7. He also argues the warrant could have specified certain devices based on the IP addresses that law enforcement had identified during the course of the investigation. *Id.*

The CASS Warrant satisfied the explicit criteria of the particularity requirement. It authorized the search and seizure of the "electronic devices" contained in Fritzinger's "barracks room [and] car" for incriminating evidence "related to . . . Article 134 (Child Pornography); Article 127 (Extortion); Article 115 (Communicating a Threat); and Article 82 (Solicitation)" of the Uniform Code of Military Justice. DE 71-2. The warrant therefore identified "the items to be seized by reference to . . . suspected criminal offense[s]." *Blakeney*, 949 F.3d at 863. And it described those items "in a manner that allow[ed] an executing officer to know precisely what he has been authorized to search for and seize," namely the electronic devices in Fritzinger's barracks room and vehicle. *See id.*

However, Fritzinger argues that the Fourth Amendment requires further specificity where law enforcement "identified specific IP addresses . . . linked to specific devices." DE 71 at 7. Just because "the warrant *could* have been more specific" does not mean that it *should* have been more specific. *See United States v. Cobb*, 970 F.3d 319, 328 (4th Cir. 2020), *as amended* (Aug. 17, 2020). "A warrant need not—and in most cases, cannot—scrupulously list and delineate each and every item to be seized." *See id.* at 327–28. Even in the context of electronic devices, "so long as the basic requirements of probable cause and particularity are met," as here, a warrant may properly authorize their retrieval and holistic review without offending the Fourth Amendment. *See id.* at 329. Thus, even a warrant authorizing the search of "all electronic devices" may be sufficiently particular where the supporting affidavit "established a sufficient connection between

the alleged crime [i.e., communicating threats of death or bodily injury] and the items sought." *See United States v. Sueiro*, 59 F.4th 132, 140 (4th Cir. 2023).

In this case, the challenged warrant did not have to "delineate each and every" device by their assigned IP addresses because searching all of the devices was a reasonable investigative measure based on the nature of the suspected offenses. *See Cobb*, 970 F.3d at 327–29; *Sueiro*, 59 F.4th at 140. As the affidavit explains, Fritzinger participated in several conversations where he would switch between several Instagram accounts within minutes to solicit additional sexually explicit photographs from target minors and threaten them with the release of their previous photographs if they failed to comply with his demands. *See* DE 71-2 at 4–5. Thus, the affidavit provided a reasonable basis to believe that the "content received as a result of these conversations may exist on [his] electronic devices" as extortion material. *Id.* at 6.

The remaining question is whether Fritzinger's electronic devices were fairly implicated for search and seizure. The affidavit stated that his cellphone can transfer large amounts of data, including sexually explicit material, to any laptop and other electronic devices for storage. *See id.* To properly search the devices for evidence and mitigate the risk of "tampering or destruction (both from external sources as well as destructive code imbedded in the system)," seizing the devices for transport to "a controlled environment is essential to [the] complete and accurate analysis" of the digital evidence in this case. *See id.* The affidavit substantially demonstrated probable cause to search and seize all of the electronic devices contained in Fritzinger's barracks room and vehicle. In this case, there was evidence that the devices were themselves instrumentalities, not merely receptacles for evidence. Accordingly, the warrant authorizing the search and seizure of the devices did not exceed the probable cause upon which it was issued.

*v. Instagram Warrant*

Fritzinger seeks to suppress the activity logs and user communications that Instagram disclosed to law enforcement pursuant to the Instagram Warrant. Fritzinger argues the warrant was insufficiently particularized with respect to the scope of those two disclosures. *See* DE 71 at 9. He argues that the warrant did not specify time-based limitations on the disclosure of activity logs pertaining to the target usernames. *Id.* He argues the warrant should have limited the activity log disclosure to the known time period for the suspected offenses, namely June 4, 2018 to April 28, 2020. *See id.* at 9–10. He also argues that, although the warrant specified time-based limitations on the disclosure of his substantive communications with other users, it did not specify "any further limitations" such as disclosing only those communications with "the accounts of those minors" whom he allegedly extorted. *See id.* Based on the breadth of these disclosures, Fritzinger contends the warrant amounted to a "'general warrant[]' without meaningful limitations." *See id.* at 10.

The Instagram Warrant was not a "general warrant" as Fritzinger suggests. General warrants "'authorize 'exploratory rummaging in a person's belongings.'" *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (quoting *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)). Officers executing general warrants could "ransack[] [a suspect's] home for four hours and cart[] away quantities of his books and papers" for evidence of any criminal conduct. *See Stanford v. Texas*, 379 U.S. 476, 483–84 (1965).

On the other hand, a sufficiently particular warrant "makes general searches under them impossible." *Id.* (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)). "By having to state with particularity the scope of the authorized search, a warrant prohibits the government from having 'unbridled discretion to rummage at will among a person's private effects.'" *United States v. Zelaya-Veliz*, 94 F.4th 321, 337 (4th Cir. 2024) (quoting *Arizona v. Gant*, 556 U.S. 332, 345 (2009)). As stated above, to prevent executing officers from enjoying unbridled discretion,

particularized warrants must meet either of two conditions: "identify[] the items to be seized by reference to a suspected criminal offense" or "describ[e] them in a manner that allows an executing officer to know precisely what he has been authorized to search for and seize." *Blakeney*, 949 F.3d at 863. The instant warrant does both.

The warrant clearly articulated the categories of information to be disclosed pertaining to seventeen usernames. *See* DE 70-7 at 14. Specifically, it required disclosures of (1) "activity logs, including IP logs and other documents showing the IP address, date, and time of each login to the account, as well as any other log file information" since account creation; and (2) "communications and other messages sent or received by the account [during the timeframe of the suspected extortion scheme]." *See id.* The warrant authorized the executing officer to seize information by reference to several suspected offenses, namely possession of child pornography, extortion, and solicitation. *See id.* at 15. It also informed the executing officer precisely what he was authorized to search for and seize, namely evidence indicating how, when, where, or by whom the associated accounts were created, accessed, or used. *See id.* at 15–16. In short, the Instagram Warrant met the explicit criteria for particularity.

Fritzinger is silent on this point. Rather, he asserts the social media disclosures are particularly invasive in this context and require time- and subject-based limitations where possible. *See* DE 71 at 8–10. To support the need for time- and subject-based limitations in the social media context, Fritzinger relies on the opinion contained in *United States v. Blake*, 868 F.3d 960 (11th Cir. 2017). However, *Blake* does not control the issue before this court.

*Blake* concerned two social media warrants that required Facebook to disclose "virtually every type of data" on the defendant's account without any time- or subject-based limitations. *Id.* at 966–67. The *Blake* court observed that the warrants "could have limited the request to messages

sent to or from persons suspected at that time of being prostitutes or customers" and "should have requested data only from the period of time during which [the defendant] was suspected of taking part in the prostitution conspiracy." *Id.* at 974. These limitations "would have undermined any claim that the Facebook warrants were the internet-era version of a general warrant." *Id.* (internal quotations marks omitted). This portion of *Blake*, however, is *dicta* and factually distinguishable.

The *Blake* court stated it "need not decide whether the Facebook warrants violated the Fourth Amendment." *Id.* at 974–75. Thus, instead of resolving the particularity issue on its merits, the court applied the good faith exception to the exclusionary rule. *See id.* Moreover, the *Blake* court evaluated the validity of a warrant that required Facebook to disclose "virtually every type of data" on the defendant's account. *See id.* at 966–67. Here, the warrant required Instagram to disclose limited portions of information associated with Fritzinger's accounts. *See* DE 70-7 at 14–15. Unlike the warrant in *Blake*, the warrant before this court cannot reasonably be construed as an "internet-era version of a general warrant" due to the limited nature of the required disclosures. *See* 868 F.3d at 974 (internal quotations marks omitted).[1]

---

[1] The Eleventh Circuit expanded on *Blake* through its recent opinion in *United States v. McCall*, 84 F.4th 1317, 1328 (11th Cir. 2023), *cert. denied*, No. 23-6609, 2024 WL 899358 (U.S. Mar. 4, 2024). *McCall* concerned a search warrant that allowed investigators to review "practically all conceivable content on the cloud account." *Id.* at 1328. The court observed that "a subject-based limitation [on communication disclosures] may sometimes be so broad as to be meaningless" because "the same [communicative] content can be stored in so many different formats." *Id.* at 1327. The court indicated "the preferred method of limiting the scope of a search warrant for a cloud account will usually be time-based. By narrowing a search to the data created or uploaded during a relevant time connected to the crime being investigated, officers can particularize their searches to avoid general rummaging." *Id.* at 1328. Although the court recognized that the use of subject- or time-limitations on cloud or data-based warrants will depend on "the circumstances of an investigation," it endorsed time-based limitations "in the mine run of cases" as "both practical and protective of privacy interests." *Id.*

Although *McCall* builds on the reasoning in *Blake*, Fritzinger does not rely on *McCall* to support his particularity challenge. Even if he did, however, *McCall* concerned another

There is no one-size-fits-all solution to satisfy the particularity requirement. As the Fourth Circuit recently observed, the need for additional time- and subject-based limitations, even in the social media context, depends on "the circumstances and type of items [or information] involved" in the investigation. *See Zelaya-Veliz*, 94 F.4th at 337 (quoting *Cobb*, 970 F.3d at 327). Accordingly, the argument for additional time- and subject-based limitations may succeed in the right context. Just not in this context.

The affidavit explained that Fritzinger used multiple Instagram accounts with shifting usernames to extort several known and unknown victims for several years. *See* DE 70-7 at 3–6. The communications during the time period of the suspected extortion activity and the activity logs documenting login requests and IP addresses would constitute evidence of the "who, what, why, when, where, and how" of the suspected extortion scheme. *Id.* at 9–10. The investigative value of the activity log disclosure, in particular, lies in the fact that "account activity can indicate who has used or controlled the Instagram account." *Id.* at 9. Based on these facts, the affidavit provided a reasonable basis for probable cause to exist to review the activity logs and communications associated with the targeted accounts.

The timeframe (or lack thereof) associated with each disclosure was also reasonable in light of the facts contained in the affidavit. The affidavit explained that the extortion activity occurred as far back as June 18, 2018. *See id.* at 5. Therefore, the timeframe for the communications disclosure substantially coincided with the known length of the extortion scheme. *See id.* at 14. As for the activity logs disclosure, the affidavit stated that account activity can help law enforcement attribute the target accounts to a common user. *See id.* at 9–10. This kind of

---

overexpansive warrant that lacked any meaningful limitations, whereas the warrant in this case limited the communications disclosure by time and required a temporally unrestrained but nonetheless reasonable activity log disclosure.

information becomes more reliable for attribution purposes when it covers a wider timeframe. Additionally, activity logs (e.g., access methods, IP addresses) do not implicate the same privacy interests as private communications between users. *See, e.g.*, *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (no privacy interest in "internet and phone 'subscriber information,'—*i.e.*, his name, email address, telephone number, and physical address"); *United States v. Soybel*, 13 F.4th 584, 591–92 (7th Cir. 2021) (no privacy interest in "individual's own IP address or the IP addresses of the websites he visits"). The nature and purpose of the activity log disclosure obviated the need for the same kind of time-based limitation imposed on the communications disclosure. In the context of the investigation against Fritzinger, the activity log and communications disclosures were reasonably particularized.

Alternatively, even if the lack of additional time- and subject-based limitations rendered the disclosures unreasonable, "the good faith exception to the exclusionary rule applies." *See Zelaya-Veliz*, 94 F.4th at 340; *McCall*, 84 F.4th at 1326. As the *Zelaya-Veliz* court stated:

> Given the unsettled nature of whether a temporal limitation is required on a warrant authorizing the search and seizure of Facebook account data, we cannot say that a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization. Rather, law enforcement here acted pursuant to a warrant that was not so facially deficient that the executing officers could not reasonably presume it to be valid.

94 F.4th at 340–41 (cleaned up). To the extent S/A Salomon, as the executing officer, relied in good faith on the Instagram Warrant, which he believed was reasonably particularized as to the investigation before him, suppression of the warrant's fruits is unwarranted.

**B. Warrant Requirement**

Fritzinger seeks to suppress the IP logs that Snap, Google, and Facebook returned pursuant to their respective subpoenas. *See* DE 71 at 10–14; DE 71-7; DE 71-9; DE 71-10. He argues that he had a "legitimate privacy interest in his IP address" under *Carpenter v. United States*, 585 U.S.

296 (2018). *See* DE 71 at 12–14; DE 79 at 5–6. Thus, he contends, the government violated the Fourth Amendment when it relied on administrative subpoenas, rather than warrants supported by probable cause, to obtain the IP logs at issue. *See* DE 71 at 14.

Searches conducted without a warrant are "per se unreasonable" and generally unconstitutional subject to a few exceptions. *See Katz v. United States*, 389 U.S. 347, 357 (1967). To qualify as a "search" under the Fourth Amendment, "the person who claims the protection . . . [must have] a legitimate expectation of privacy in the invaded place." *United States v. Castellanos*, 716 F.3d 828, 833 (4th Cir. 2013) (citation omitted). The defendant must show (1) a "subjective expectation of privacy" that is (2) "objectively reasonable; in other words, it must be an expectation that society is willing to recognize as reasonable." *Id.* (quoting *United States v. Bullard*, 645 F.3d 237, 242 (4th Cir. 2011)). "The burden of showing a legitimate expectation of privacy in the area searched rests with the defendant." *Id.*

Fritzinger overlooks his burden of proof with respect to the subjective element of his privacy claim. A defendant seeking to establish a cognizable privacy interest must demonstrate that he "intentionally took steps to avoid allowing the public at large to access pertinent evidence." *See, e.g.*, *United States v. Chavez*, 423 F. Supp. 3d 194, 201 (W.D.N.C. 2019) (cleaned up); *United States v. Ramapuram*, 632 F.2d 1149, 1154 (4th Cir. 1980) (explaining the court must ask "whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy,'. . . whether, in the words of the *Katz* majority, the individual has shown that 'he seeks to preserve (something) as private'" (citations omitted)).

Fritzinger does not allege he took any steps to protect his IP address from disclosure to his service providers or that he believed his IP address would remain undisclosed to the public at large. Nevertheless, the court declines to resolve the motion at this step of the analysis. Fritzinger

maintains that he "has a legitimate expectation of privacy" in his IP address, DE 71 at 12, and the United States offers no contrary position specifically with respect to the subjective element of his privacy claim. The court thus "assume[s]" Fritzinger had an "actual subjective expectation of privacy." *See Ramapuram*, 632 F.2d at 1155.

Whether that privacy expectation was objectively reasonable is the focus of the parties' dispute. Fritzinger asserts that his privacy expectation is objectively reasonable under *Carpenter*. In his view, IP addresses and CSLI are analogous because their disclosures coincide with widespread and almost necessary cellphone use and have the capacity to facilitate user geolocation. *See* DE 71 at 12–14; DE 79 at 5–6. The United States disputes the analogy. It asserts that users must take affirmative steps to connect to the internet and thereby provide their IP addresses to third parties like Snap, Google, and Facebook, and that IP addresses are not as accurate or useful as CSLI for geolocation or tracking purposes. *See* DE 75 at 13.

The court has concerns about the use of investigatory subpoenas in this case. These subpoenas allowed law enforcement to review a chronicle of IP addresses associated with each request to access the targeted social media accounts. DE 71-8; DE 71-11. Although, as the United States points out, most circuits have rejected the general proposition that IP addresses are objectively private information even after *Carpenter*, *see* DE 75 at 12 (collecting cases), a major factor giving rise to this consensus is the limited nature of the information at issue for purposes of historical tracking. *See, e.g.*, *United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019); *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018); *United States v. Soybel*, 13 F.4th 584, 592–93 (7th Cir. 2021); *United States v. Shipton*, 5 F.4th 933, 936 (8th Cir. 2021); *United States v. Trader*, 981 F.3d 961, 968 (11th Cir. 2020). However, accurate and retrospective IP geolocation methods appear to be "improving over the years, especially at the city level, despite the constant changes

in the address space." *See* Dan Komosny, *Retrospective IP Address Geolocation for Geography-Aware Internet Services*, 21 Sensors 4975 (2021), https://doi.org/10.3390/s21154975. As these methods improve in accuracy and reliability, IP logs could allow law enforcement to "travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers." *Carpenter*, 585 U.S. at 312.

This court does not have the record before it to decide whether Fritzinger's privacy expectation in his IP logs was objectively reasonable. Fortunately, the court need not do so. When confronted with "novel questions posed by digital technology," the Fourth Circuit has advised courts "to proceed with caution." *See United States v. Zelaya-Veliz*, 94 F.4th 321, 340 (4th Cir. 2024). "Courts should not punish law enforcement officers who are on the frontiers of new technology simply because they are at the beginning of a learning curve and have not yet been apprised of the preferences of courts on novel questions." *See id.* at 341. Even assuming that the challenged subpoenas gave rise to an unconstitutional search, S/A Salomon relied in good faith belief on the validity of 18 U.S.C. § 2703, 10 U.S.C. § 846, and the prevailing judicial consensus as described above to obtain the IP logs. *See* DE 71-7; DE 71-9; DE 71-10; DE 75 at 14. Accordingly, the good faith exception to the exclusionary rule applies, and the IP logs shall not be suppressed. *See United States v. Taylor*, 54 F.4th 795, 804–05 (4th Cir. 2022) ("[A]n exception to the exclusionary rule exists where government agents acted with an objectively reasonable good faith belief that their conduct was lawful." (internal quotation marks omitted)).

**C. Motion in Limine**

Fritzinger argues that the court should prohibit the government from introducing "all communications" made by nontestifying third parties, namely screenshots of victim profiles revealing their age, because those statements constitute hearsay not subject to any exception. DE 71 at 14. However, the United States argues that the "motion is largely premature, with trial

months away and no foundation laid in court to support any such exhibits." DE 75 at 14. The government also confirms that it would use the evidence as proof of Fritzinger's "intent, lack of mistake, and modus operandi," rather than to prove the truth of the matter asserted. *Id.* at 14–15. Based on the parties' respective positions, the court denies Fritzinger's motion in limine without prejudice as to reconsideration upon further development of the evidence during trial.

**III. Conclusion**

For the foregoing reasons, Defendant's motion to suppress evidence [DE 71] is DENIED. This matter shall proceed to trial, which is currently scheduled to begin September 9, 2024.

SO ORDERED this 10th day of July, 2024.

Richard E Myers II

RICHARD E. MYERS II
CHIEF UNITED STATES DISTRICT JUDGE